Amendments to the Claims

This listing of the claims will replace all prior versions, and listings of claims in the application:

Listing of Claims

1. (Currently amended) A method for controlling access to a network, the method comprising the following steps:

(a) coupling a user device to a network;

(b) transmitting a first response including a particular secret of at least two secrets stored in the user device to the network;

(c) generating a second response including the particular secret upon receipt of the first response by the network;

(d) comparing the first response and second response; and

(e) authenticating the user device if the first response and second response match, and not authenticating the user device if the first response and second do not match.

2. (Currently amended) The method of claim 1 wherein the first response includes a public shared secret as the particular secret.

3. (Currently amended) The method of claim 1 wherein the first response includes a private shared secret as the particular secret.

4. (Currently amended) The method of claim 1 wherein the first response includes a public shared secret and a private shared secret as the particular secret.

5. (Original) The method of claim 1 wherein the second response includes a public shared secret.

6. (Original) The method of claim 1 wherein the second response includes a private shared secret.

7. (Original) The method of claim 1 wherein the second response is generated by the network.

8. (Currently amended) A method for controlling access to a network, the method comprising the following steps:

(a) coupling a user device storing at least two secrets to a network;

(b) transmitting a request to the network;

(c) transmitting a challenge including an instruction to use a particular secret of the secrets to the user device;

(d) generating a first response including the particular secret;

(e) transmitting the first response to the network;

(f) generating a second response including the particular secret upon receipt of the first response by the network;

(g) comparing the first response and second response; and

(h) authenticating the user device if the first response and second response match, and not authenticating the user device if the first response and second do not match.

9. (Currently amended) The method of claim 8 wherein the first response includes a symmetric public shared secret in the particular secret.

10. (Currently amended) The method of claim 8 wherein the first response includes a symmetric private shared secret in the particular secret.

11. (Currently amended) The method of claim 8 wherein the first response includes a symmetric public shared secret in the particular secret and a symmetric private shared secret in the particular secret.

12. (Currently amended) The method of claim 8 wherein the second response includes a symmetric public shared secret in the particular secret.

13. (Currently amended) The method of claim 8 wherein the second response includes a symmetric private shared secret in the particular secret.

14. (Original) The method of claim 8 wherein the second response is generated by the network.

15. (Currently amended) A method for controlling access to a public network, the method comprising the following steps:

(a) coupling a user device to a public network, the network including a server, and the user device stores at least two public shared secrets;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to ascertain one of the public shared secrets as a selected public shared secret stored on the user device;

(e) generating a first response using at least the selected public shared secret;

(f) transmitting the first response to the server;

(g) generating a second response upon receipt of the first response by the server;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the public network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

16. (Original) The method of claim 15 wherein the first response includes a symmetric public shared secret.

17. (Original) The method of claim 15 wherein the second response includes a symmetric public shared secret.

18. (Original) The method of claim 8 wherein the second response is generated by the server.

19. (Currently amended) A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including a server, and the user device stores at least two private shared secrets;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to ascertain at least a selected private shared secret stored on the user device;

(e) generating a first response using at least the selected private shared secret as one of the private shared secrets;

(g) transmitting the first response to the server;

(h) generating a second response upon receipt of the first response by the server;

(i) comparing the first response and second response; and

(j) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

20. (Currently amended) A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including an access control server, and the user device stores at least two private shared secrets and at least two public shared secrets;

(b) transmitting an access request from the user device to the server, the access request comprising a first response that includes a selected public shared secret as one of the public shared secrets and a selected private shared secret as one of the private shared secrets, both stored on the user device;

(c) invoking the server to generate a second response upon receipt of the first response, the server generating the second response by means of the following steps,

(i) processing the challenge transmitted to the user device to retrieve the selected public shared secret and the selected private shared secret, and

(ii) processing the selected public shared secret and selected private shared secret to generate the second response;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first

response and second do not match.

21. (Original) The method of claim 20 wherein the first response includes a symmetric public shared secret and a symmetric private shared secret.

22. (Original) The method of claim 20 wherein the second response includes a symmetric public shared secret and a symmetric private shared secret.

23. (Currently amended) A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including an access control server, and the user device stores at least two private shared secrets and at least two public shared secrets;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to retrieve a selected public shared secret and a selected private shared secret stored on the user device;

(e) processing the selected public shared secret and selected private shared secret to generate a first response;

(f) transmitting the first response to the server;

(g) invoking the server to generate a second response upon receipt of the first response by the server, the server generating the second response by means of the following steps,

(i) processing the challenge transmitted to the user device to retrieve the selected public shared secret and the selected private shared secret, and

(ii) processing the selected public shared secret and selected private shared secret to generate the second response;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.